

CONTROL THEOREMS FOR ABELIAN VARIETIES OVER FUNCTION FIELDS

KI-SENG TAN

ABSTRACT. We prove control theorems for abelian varieties over function fields.

1. INTRODUCTION

Control theorems for abelian varieties over \mathbb{Z}^d -extensions of global (or local) fields aim at giving estimates for the sizes of their Galois (or flat) cohomology groups. They play a crucial role in the arithmetic of abelian varieties and have important application to Iwasawa theory. Control theorems are well known over number fields. In this paper we prove control theorems for abelian varieties over function fields.

Our first result is the following. Let p denote a given prime number and let q be a power of p . We denote by \mathbb{F}_q the finite field of order q .

Theorem 1.1. (The Local Control Theorem) *Let A be an abelian variety over the local field $K = \mathbb{F}_q((T))$. Assume that the reduction \bar{A} of A modulo (T) is an ordinary abelian variety. Write $\bar{A}(\mathbb{F}_q)_p$ for the p -Sylow subgroup of $\bar{A}(\mathbb{F}_q)$. Then for any \mathbb{Z}_p^d -extension L/K , we have the following estimate on the size of the Galois cohomology group:*

$$|H^1(L/K, A(L))| \leq |\bar{A}(\mathbb{F}_q)_p|^{d+1}.$$

Similar result over local fields of characteristic zero has been proved by Mazur ([Maz72]) and Greenberg ([Gre03]). These proofs depend on deep theorems on local points of abelian varieties. However, some of these theorems may not hold in characteristic p . For example, one remarkable phenomenon is that the p -completion of the rational points of an abelian variety over a local field of characteristic p is not a finitely generated \mathbb{Z}_p -module. Our proof (in section 3) introduces a new technique involving a huge purely inseparable extension and hence works well in the characteristic p situation.

Given an abelian variety A over a field K of characteristic p , we regard A as a sheaf for the flat topology on K and denote the kernel of the multiplication by p^m on A by $\mathcal{A}[p^m]$. If K is a global field, the p^m -Selmer group $\text{Sel}_{p^m}(F)$ for a finite extension field F of K is defined

Acknowledgement: This research was supported in part by the National Science Council of Taiwan, NSC95-2115-M-002-017-MY2.

to be the kernel of the composition

$$H^1(F, \mathcal{A}[p^m]) \longrightarrow H^1(F, A) \xrightarrow{loc} \bigoplus_v H^1(F_v, A),$$

where loc is the localization map and in the direct sum, v runs through all places of F . The direct limit of $\text{Sel}_{p^m}(F)$ as $m \rightarrow \infty$ is denoted by $\text{Sel}_{p^\infty}(F)$. For any Galois extension L/K , the p -primary part of the Selmer group of A over L is taken to be the direct limit of $\text{Sel}_{p^\infty}(F)$ over all finite intermediate fields F of L/K . We write Γ_F for the Galois group of L/F and let

$$\text{res}_{L/F} : \text{Sel}_{p^\infty}(F) \longrightarrow \text{Sel}_{p^\infty}(L)^{\Gamma_F}$$

be the restriction map. We deduce from Theorem 1.1 the following control theorem.

Theorem 1.2. (The Control Theorem) *Let L be a \mathbb{Z}_p^d -extension of a global field K of characteristic p with Galois group $\text{Gal}(L/K) = \Gamma$. Assume that L/K is unramified outside a finite set S of places of K . Let A be an abelian variety over K with good ordinary reduction at every place in S . Then for every finite intermediate extension F of L/K , the kernel and the cokernel of the restriction map $\text{res}_{L/F}$ on the p -primary Selmer groups $\text{Sel}_{p^\infty}(F)$ are finite. Furthermore, if $d = 1$, then the orders of the kernel and the cokernel of $\text{res}_{L/F}$ are bounded as F varies.*

The number field counterpart of this theorem appears in Mazur ([Maz72]) and Greenberg ([Gre03]).

To show that our control theorem is very useful we give an application to Iwasawa theory. Denote by Λ_Γ the Iwasawa algebra $\mathbb{Z}_p[[\Gamma]]$ and denote the Pontryagin dual $\text{Hom}(\text{Sel}_{p^\infty}(L), \mathbb{Q}_p/\mathbb{Z}_p)$ by X_L .

Theorem 1.3. *If the condition of Theorem 1.2 holds, then X_L is a finitely generated module over Λ_Γ .*

This theorem is fundamental for advances in Iwasawa theory. Such results in the function field case only appear recently. Lacking our local control theorem, these results have to depend on extra assumptions. For example, in Ochiai and Trihan ([OTr06, OTr08]), they assume that L/K is the constant \mathbb{Z}_p -extension unramified at every place of K , while Bandini and Longhi ([BL06]) treat the case of elliptic curve with split multiplicative reduction at every place of S . On the other hand, our control theorem reduces the proof of Theorem 1.3 to a routine task, because it obviously implies that the p -torsion subgroup $\text{Sel}_{p^\infty}(L)^{\Gamma}[p]$ of $\text{Sel}_{p^\infty}(L)^{\Gamma}$ is a finite group and hence the Nakayama Lemma (see [Was82], p.279) can be applied to the compact Λ_Γ -module X_L . Here is another application of our main results, which strengthen Theorem 1.1 of [BL06].

Theorem 1.4. *Suppose that A/K is an elliptic curve and at every place $v \in S$, A has either good ordinary or split multiplicative reduction. Then X_L is a finitely generated Λ_Γ -module.*

In Section 2.3 we prove our main result Theorem 1.2 as well as Theorem 1.4, assuming Theorem 1.1 whose proof we postpone to Section 3.4.

Finally, we set some notations. From now on, every field will be of characteristic $p > 0$. For an abelian variety A defined over a field K , denote by $A[p^m]$ the p^m -torsion points on A and write $A[p^\infty] = \bigcup_m A[p^m]$. Denote $A(K)_{\text{tor},p} = A[p^\infty] \cap A(K)$, the p -primary part of $A(K)_{\text{tor}}$.

Suppose that K is a local field. We use \mathbb{F}_K to denote its residue field which can also be viewed as its constant field. Let $A^1(K)$ denote the pro- p subgroup of $A(K)$ consisting of points with trivial reduction, and let $A(K)_p$ denote the maximal pro- p subgroup of $A(K)$.

For a global or local field K and for each n , we use $K^{(1/p^n)}/K$ to denote the unique purely inseparable extension of degree p^n . Also, we use \bar{K} to denote the separable closure of K and write $G_K = \text{Gal}(\bar{K}/K)$. We write $\bar{K}^{(1/p^n)}$ for $\overline{K^{(1/p^n)}}$. Thus, the algebraic closure of K equals $\bar{K}^{(1/p^\infty)} := \bigcup_{n=1}^\infty \bar{K}^{(1/p^n)}$. The Frobenius substitution

$$\text{Frob}_{p^n} : K^{(1/p^n)} \longrightarrow K, \quad x \mapsto x^{p^n},$$

is an isomorphism. And we use it to identify $G_{K^{(1/p^n)}}$, for $n = 1, \dots, \infty$, with G_K .

The author would like to thank A. Bandini, W.-C. Chi, C. D. González-Avilés, K.F. Lai, D. Rockmore and F. Trihan for many valuable suggestions.

2. THE p^m -TORSION POINTS

In this section, we prove that Theorem 1.1 implies Theorem 1.2 and Theorem 1.4.

2.1. Ordinary abelian varieties. Assume that K is a field of characteristic p and A/K is an abelian variety of dimension g . Then A/K is ordinary if and only if (over the algebraic closure of K) the group scheme $\mathcal{A}[p]$ can be decomposed as (cf. [Mum74], Sec. 14):

$$\mathcal{A}[p] = (\mathbb{Z}/p\mathbb{Z})^g \times (\mu_p)^g. \quad (1)$$

This condition is equivalent to

$$A[p^m] \simeq (\mathbb{Z}/p^m\mathbb{Z})^g. \quad (2)$$

In this case, the multiplication by p on A is decomposed as

$$[p] = V \circ F, \quad (3)$$

where $F : A \longrightarrow A^{(p)}$ is the Frobenius isogeny and $V : A^{(p)} \longrightarrow A$ is separable.

Lemma 2.1. *Let A be an abelian variety over a local field K so that \bar{A} , the reduction of A , is an ordinary abelian variety. Then A is also ordinary and the reduction map induces an isomorphism of G_K -modules:*

$$A[p^\infty] \xrightarrow{\sim} \bar{A}[p^\infty] \quad (4)$$

Here G_K acts on $A[p^\infty]$ through its action on $\bar{K}^{(1/p^\infty)}$ and its action on $\bar{A}[p^\infty]$ factors through the quotient map $G_K \longrightarrow \text{Gal}(\bar{\mathbb{F}}_K/\mathbb{F}_K)$.

Proof. Let m be any given positive integer. By replacing K with a suitable finite (maybe inseparable) extension field of it, we may assume that $A[p^m]$ is rational over K and $\bar{A}[p^m]$ is rational over \mathbb{F}_K . Let \mathcal{O} be the ring of integers of K and denote by \mathbf{A} the Néron model of A over \mathcal{O} . Since $\mathbf{A}[p^m] := \ker(\mathbf{A} \xrightarrow{p^m} \mathbf{A})$ is proper, quasi-finite and hence finite over \mathcal{O} and \mathcal{O} is a complete discrete valuation ring, we have $\mathbf{A}[p^m] = \text{spec } B$ with $B = \prod B_i$ where each B_i is a local ring over \mathcal{O} ([Mil80] I.4.2(b)). Since $\bar{A}[p^m]$ is rational over \mathbb{F}_K , the residue field of each B_i equals \mathbb{F}_K and hence the reduction map from $\text{Hom}_{\mathcal{O}}(B, \mathcal{O}) = \text{Hom}_{\mathcal{O}}(B, K) = A[p^m]$ to $\text{Hom}_{\mathcal{O}}(B, \mathbb{F}_K) = \bar{A}[p^m]$ is surjective. The lemma is proved, since $\bar{A}[p^m] \simeq (\mathbb{Z}/p^m\mathbb{Z})^g$ and the order of $A[p^m]$ is at most p^{gm} . \square

Corollary 2.1. *Let A be an abelian variety over a local field K with good ordinary reduction and let L be a local field containing K . Then the following hold:*

- (a): *If P is a point in $A(L)$, then all the p^m -division points of P are contained in $A(\bar{L}^{(1/p^m)})$. In particular, the p^m -torsion points $A[p^m] \subset A(\bar{K}^{(1/p^m)})$.*
- (b): *If L/K is separable, then the group $A(L)_{\text{tor},p}$ is unramified over K , in the sense that every point in $A(L)_{\text{tor},p}$ is rational over the maximal unramified sub-extension of L/K .*
- (c): *The subgroup $A^1(L) \subset A(L)$ is a torsion free \mathbb{Z}_p -module.*
- (d): *For each $P \in A^1(L)$ there is a unique $P' \in A^1(L^{(1/p^m)})$ such that $p^m P' = P$, and vice versa. In other words, we have*

$$A^1(L) = p^m A^1(L^{(1/p^m)}). \quad (5)$$

- (e): *Let $A(L^{(1/p^\infty)})_p := \bigcup_m A(L^{(1/p^m)})_p$. Then*

$$A(L^{(1/p^\infty)})_p = A^1(L^{(1/p^\infty)}) \times A(L^{(1/p^\infty)})_{\text{tor},p}, \quad (6)$$

and

$$A(L^{(1/p^\infty)})_{\text{tor},p} \simeq \bar{A}(\mathbb{F}_L)_p. \quad (7)$$

If L/K is Galois, then these are G_K -isomorphisms.

Proof. The statement (a) is directly from the arguments given before the lemma, while (b) and (c) are from the G_K -isomorphism (4).

To see (d), let $Q \in A(\bar{L}^{(1/p^m)})$ be a p^m -division point of $P \in A^1(L)$. Since the reduction \bar{Q} is contained in $\bar{A}[p^m]$, there is a point $R \in$

$A[p^m] \subset A(\bar{L}^{(1/p^m)})$ such that $P' := Q - R \in A^1(\bar{L}^{(1/p^m)})$. Obviously, P' is also a p^m -division point of P , and for $\sigma \in G_L$, we have (from (c))

$$\sigma P' - P' \in A[p^m] \cap A^1(\bar{L}^{(1/p^m)}) = \{0\}.$$

To prove (e), for each m we consider the following commutative diagram of exact sequences induced from reduction maps:

$$\begin{array}{ccccccc} 0 & \longrightarrow & A^1(L) & \longrightarrow & A(L)_p & \longrightarrow & \bar{A}(\mathbb{F}_L)_p \longrightarrow 0 \\ & & \downarrow & & \downarrow & & \parallel \\ 0 & \longrightarrow & A^1(L^{(1/p^m)}) & \longrightarrow & A(L^{(1/p^m)})_p & \longrightarrow & \bar{A}(\mathbb{F}_L)_p \longrightarrow 0, \end{array}$$

where the down-arrows are natural inclusions. Suppose $Q \in A(L)_p$ so that its reduction $\bar{Q} \in \bar{A}(\mathbb{F}_L)_p$ has order p^n , and let $P = p^n Q \in A^1(L)$. According to (d), there is a $P' \in A^1(L^{(1/p^n)})$ such that $p^n P' = P$. Then the point $Q - P'$ is contained in $A(L^{(1/p^n)})_{\text{tor},p}$ and the assignment $\bar{Q} \mapsto Q - P'$ define a natural isomorphism from $\bar{A}(\mathbb{F}_L)_p$ to $A(L^{(1/p^m)})_{\text{tor},p}$ for large m . Thus, if m is large enough, then there is a natural splitting of the exact sequence

$$0 \longrightarrow A^1(L^{(1/p^m)}) \longrightarrow A(L^{(1/p^m)})_p \longrightarrow \bar{A}(\mathbb{F}_L)_p \longrightarrow 0.$$

Thus, we obtain (6) and (7) by letting $m \rightarrow \infty$. \square

Next, we consider the case where the abelian variety A is defined over a global field K of characteristic p . Let L/K be a \mathbb{Z}_p^d -extension unramified outside a finite set S of places of K . Let Γ_0 denote the stabilizer of $A(L)_{\text{tor},p}$ for the action of $\Gamma := \text{Gal}(L/K)$ and let L_0 denote the fixed field of Γ_0 . We call a pro- p Galois extension pro- p cyclic if its Galois group is either finite cyclic or isomorphic to \mathbb{Z}_p .

Lemma 2.2. *Let notations be as above. Assume that one of the following holds:*

- (1) *A has good, ordinary reduction at every place $v \in S$.*
- (2) *A is an elliptic curve with good, ordinary or split multiplicative reduction at every place of S .*

Then there is a finite intermediate extension $K_0/K \subset L_0/K$ such that L_0/K_0 is a pro- p cyclic extension.

Proof. Note that if A has good, ordinary reduction at a place v , then A/K_v is ordinary and hence $K_v L_0$ is unramified over K_v (Corollary 2.1(b)). Also, if A is an elliptic curve with split multiplicative reduction at some $v \in S$ so that the Tate's curve has period $Q \in K_v^*$, then $K_v L_0 = \overline{K_v} \cap (\cup_{n=1}^{\infty} K_v(Q^{1/p^n})) = K_v$. This shows that L_0/K is everywhere unramified.

We then apply the global class field theory (c.f. [Tat67]) which tells us that the Galois group $W_{K,p}$ of the maximal everywhere unramified pro- p abelian extension of K fits into an exact sequence

$$0 \longrightarrow C_{K,p} \longrightarrow W_{K,p} \xrightarrow{\deg} \mathbb{Z}_p \longrightarrow 0,$$

where $C_{K,p}$ is the p -Sylow subgroup of the class group of K and \deg is induced from the degree map on the group of ideles. We choose a subgroup $W_0 \simeq \mathbb{Z}_p$ of $W_{K,p}$ and choose K_0 to be the fixed field of W_0 under the action of $W_{K,p}$ on L_0 . \square

2.2. Cohomology groups of the torsion points. In the next step, our goal is to bound, for $i = 1, 2$, the order of the cohomology group $H^i(L'/K, A(L')_p)$, where L'/K is a finite intermediate field extension of some given \mathbb{Z}_p^d -extension. To achieve this goal, we first establish the following lemma in which G is a finite p -abelian group with d generators acting on a finite p -abelian group M . We assume that there is a subgroup $H_0 \subset G$ such that G/H_0 is cyclic and $M^{H_0} = M$.

Lemma 2.3. *Let notations and conditions be as above. Then we have*

$$|H^1(G, M)| \leq |M^G|^d, \quad (8)$$

and

$$|H^2(G, M)| \leq |M^G|^{d^2}. \quad (9)$$

Proof. Consider the inflation-restriction exact sequence:

$$0 \longrightarrow H^1(G/H_0, M^{H_0}) \longrightarrow H^1(G, M) \xrightarrow{res} H^1(H_0, M)^{G/H_0}.$$

We shall bound the orders of $\ker(res)$ and $\text{Im}(res)$. Since G/H_0 is cyclic, by computing the Herbrand quotient, we see that the order of $H^1(G/H_0, M^{H_0})$ equals $|M^G/\mathcal{N}|$, where \mathcal{N} is the image of the norm map $N_{G/H_0} : M = M^{H_0} \longrightarrow M^G$. Also, since M is fixed by the action of H_0 , we have

$$H^1(H_0, M)^{G/H_0} = \text{Hom}(H_0, M^G).$$

To proceed further, choose a basis e_1, \dots, e_c of G , for some $c \leq d$, so that $e'_1 := p^m e_1, e_2, \dots, e_c$, for some non-negative integer m , form a basis of H_0 . The cocycle condition implies that if ρ is a 1-cocycle representing a class in $H^1(G, M)$, then the value $\rho(e'_1)$ equals $N_{G/H_0}(\rho(e_1))$. This implies that the image of res must be contained in the subgroup

$$\{\phi \in \text{Hom}(H_0, M^G) \mid \phi(e'_1) \in \mathcal{N}\},$$

whose order is bounded by $|M^G|^{c-1} \cdot |\mathcal{N}|$. Therefore, the inequality (8) holds, since

$$|\ker(res)| \cdot |\text{Im}(res)| \leq |M^G/\mathcal{N}| \cdot |M^G|^{c-1} \cdot |\mathcal{N}|.$$

We prove the inequality (9) by induction on d . The case where $d = 1$ is easy, since $H^2(G, M) = M^G/N_G(M)$. If $d > 1$, we choose a cyclic subgroup $H_1 \subset H_0$ such that G/H_1 is generated by $d - 1$ elements. According to the associated Hochschild-Serre spectral sequence (cf. [Sha72]), we have exact sequences

$$0 \longrightarrow E_1^2 \longrightarrow H^2(G, M) \longrightarrow H^2(H_1, M)^{G/H_1}$$

and

$$H^2(G/H_1, M^{H_1}) \longrightarrow E_1^2 \longrightarrow H^1(G/H_1, H^1(H_1, M)).$$

Therefore, the desired bound for the order of $H^2(G, M)$ can be derived from the following lemma. \square

Lemma 2.4. *Under the above assumptions, we have*

$$|H^2(G/H_1, M^{H_1})| \leq |M^G|^{(d-1)^2}, \quad (10)$$

$$|H^1(G/H_1, H^1(H_1, M))| \leq |M^G|^{d-1}, \quad (11)$$

$$|H^2(H_1, M)^{G/H_1}| \leq |M^G|^d. \quad (12)$$

Proof. The inequality (10) is in fact the induction hypothesis. To show (11), we first note that since H_1 is cyclic and acting trivially on M , the group $N := H^1(H_1, M)$ satisfies $N^G = \text{Hom}(H_1, M^G)$ and $|N^G| \leq |M^G|$. In view of this, we see that the inequality (8) for the case where the pair $(G, M) = (G/H_1, N)$ implies (11).

Again, since H_1 is cyclic, acting trivially on M , we have

$$H^2(H_1, M)^{G/H_1} = (M/p^l M)^{G/H_1},$$

where p^l is the order of H_1 . To bound the order of this group, we consider the exact sequence

$$M^G \longrightarrow (M/p^l M)^{G/H_1} \longrightarrow H^1(G/H_1, p^l M^G),$$

which is induced from

$$0 \longrightarrow p^l M \longrightarrow M \longrightarrow M/p^l M \longrightarrow 0.$$

We have

$$|H^1(G/H_1, p^l M^G)| = |\text{Hom}(G/H_1, p^l M^G)| \leq |M^G|^{d-1}.$$

\square

Corollary 2.2. *Suppose that K is a local field of characteristic p , L/K is a \mathbb{Z}_p^d -extension and A/K is an abelian variety with good, ordinary reduction. Then for every finite intermediate extension $L'/K \subset L/K$ we have*

$$|H^1(L'/K, A(L')_{\text{tor}, p})| \leq |A(K)_{\text{tor}, p}|^d,$$

and

$$|H^2(L'/K, A(L')_{\text{tor}, p})| \leq |A(K)_{\text{tor}, p}|^{d^2}$$

Proof. Corollary 2.1(b)) says that $A(L)_{\text{tor}, p}$ is unramified. Let L_0/K be the maximal unramified subextension of L/K and put $G = \text{Gal}(L'/K)$, $H_0 = \text{Gal}(L'/L_0 \cap L')$. Then apply Lemma 2.3. \square

Corollary 2.3. *Suppose that A, K, L satisfy the condition of Lemma 2.2. Let F/K be a finite intermediate extension of L/K . Then for all intermediate extension $L'/F \subset L/F$, the orders of $H^1(L'/F, A(L')_{\text{tor}, p})$ and $H^2(L'/F, A(L')_{\text{tor}, p})$ are bounded. Furthermore, if $d = 1$, then the bounds can be chosen to be independent of F .*

Proof. Let $K_0 \subset L_0 \subset L$ be as in Lemma 2.2. Without loss of generality, we may assume that $F = K$ for the proof of the first statement. Put $K'_0 = L' \cap K_0$, $G = \text{Gal}(L'/K'_0)$ and $H_0 = \text{Gal}(L'/L_0 \cap L')$. Obviously, $A(K'_0)_{\text{tor},p}$ is contained in $A(K_0)_{\text{tor},p}$. Therefore, from Lemma 2.3 we see that for $j = 0, 1, 2$ the order of the $\text{Gal}(K'_0/K)$ -module $H^j(L'/K'_0, A(L')_{\text{tor},p})$ is bounded by $|A(K_0)_{\text{tor},p}|^{d^j}$ which is independent of L' . This implies that the orders $|H^i(K'_0/K, H^j(L'/K'_0, A(L')_{\text{tor},p}))|$, for $i + j = 1, 2$, are also bounded. Then we use the Hochschild-Serre spectral sequence

$$H^i(K'_0/K, H^j(L'/K'_0, A(L')_{\text{tor},p})) \implies H^{i+j}(L'/K, A(L')_{\text{tor},p})$$

to verify the first statement.

Now consider the case where $d = 1$. Let K_n be the n th layer of L/K . Using Herbrand quotient, we see that for $F = K_n$,

$$|H^1(L'/F, A(L')_{\text{tor},p})| = |H^2(L'/F, A(L')_{\text{tor},p})| \leq |A(K_n)_{\text{tor},p}|.$$

This bound increases with n . To find a bound independent of n , we first note that $A(L)_{\text{tor},p}$ is cofinite over \mathbb{Z}_p and consider the p -divisible part $A(L)_{\text{tor},\infty}$ of $A(L)_{\text{tor},p}$. Let T denote the finite quotient $A(L)_{\text{tor},p}/A(L)_{\text{tor},\infty}$, and let n_0 be a positive integer such that if $n \geq n_0$, then $A(K_n)_{\text{tor},p}$ contains $A[p^2] \cap A(L)_{\text{tor},p}$.

Suppose $n \geq n_0$ and $Q \in A(K_n) \cap A(L)_{\text{tor},\infty}$. It is easy to see that there is a $Q' \in A(K_{n+1}) \cap A(L)_{\text{tor},\infty}$ such that $pQ' = Q$ and for every $\sigma \in \text{Gal}(K_{n+1}/K_n)$, the point $P_\sigma := {}^\sigma Q' - Q'$ is contained in $A[p] \cap A(L)_{\text{tor},\infty}$. Note that $A[p] \cap A(L)_{\text{tor},\infty}$ is a subgroup of $p(A(K_n) \cap A(L)_{\text{tor},\infty})$ which is contained in $N_{K_{n+1}/K_n}(A(K_{n+1}) \cap A(L)_{\text{tor},\infty})$. Also, Q can be expressed as the difference $N_{K_{n+1}/K_n}(Q') - \sum_{\sigma \in \text{Gal}(K_{n+1}/K_n)} P_\sigma$. Therefore, Q is contained in $N_{K_{n+1}/K_n}(A(K_{n+1}) \cap A(L)_{\text{tor},\infty})$. This shows that

$$A(K_n) \cap A(L)_{\text{tor},\infty} \subset N_{K_m/K_n}(A(K_m) \cap A(L)_{\text{tor},\infty}), \text{ if } m \geq n.$$

Therefore, we have, for $F = K_n$, $L' = K_m$, $m \geq n \geq n_0$,

$$|H^2(L'/F, A(L')_{\text{tor},p})| = |A(K_n)_{\text{tor},p}/N_{K_m/K_n}(A(K_m)_{\text{tor},p})| \leq |T|.$$

We can choose $|T|$ as the desired bound. \square

2.3. The proofs of Theorem 1.2 and Theorem 1.4. We first prove that Theorem 1.1 implies Theorem 1.2. Let $S(F)$ denote the set of places of F sitting over S . Let L'/F be a finite intermediate extension of L/F and put $G = \text{Gal}(L'/F)$. For $m = 1, 2, \dots, \infty$, consider the restriction map

$$\text{res}_m : H^1(F, \mathcal{A}[p^m]) \longrightarrow H^1(L', \mathcal{A}[p^m])^G,$$

and define

$$\text{Sel}_{p^\infty}(L'/F) := \{\eta \in H^1(F, \mathcal{A}[p^\infty]) \mid \text{res}_\infty(\eta) \in \text{Sel}_{p^\infty}(L')\}.$$

Then $\text{Sel}_{p^\infty}(F) \subset \text{Sel}_{p^\infty}(L'/F)$ and for the restriction map

$$\text{res}_{L'/F} : \text{Sel}_{p^\infty}(F) \longrightarrow \text{Sel}_{p^\infty}(L')^G,$$

we have the inequalities:

$$|\ker(\text{res}_{L'/F})| \leq |\ker(\text{res}_\infty)|, \quad (13)$$

and

$$|\text{coker}(\text{res}_{L'/F})| \leq |\text{coker}(\text{res}_\infty)| \cdot |\text{Sel}_{p^\infty}(L'/F) : \text{Sel}_{p^\infty}(F)|. \quad (14)$$

For every m apply the Hochschild-Serre spectral sequence ([Mil80], p. 105)

$$\mathrm{H}^i(G, \mathrm{H}^j(L', \mathcal{A}[p^m])) \implies \mathrm{H}^{i+j}(F, \mathcal{A}[p^m]).$$

The spectral sequence says that $\ker(\text{res}_m)$ equals $\mathrm{H}^1(G, \mathcal{A}[p^m](L'))$ and $\text{coker}(\text{res}_m)$ is isomorphic to a subgroup of $\mathrm{H}^2(G, \mathcal{A}[p^m](L'))$. We have $\mathcal{A}[p^m](L') = A(L')[p^m]$, which equals $A(L')_{\text{tor}, p}$ for m large enough. By letting m go to ∞ and by applying Corollary 2.3, we conclude that the orders $|\ker(\text{res}_\infty)|$, $|\text{coker}(\text{res}_\infty)|$ are finite and they are bounded if $d = 1$ and F varies.

To bound the index $|\text{Sel}_{p^\infty}(L'/F) : \text{Sel}_{p^\infty}(F)|$, we use the exact sequence

$$\text{Sel}_{p^\infty}(F) \longrightarrow \text{Sel}_{p^\infty}(L'/F) \longrightarrow \bigoplus_v \mathrm{H}^1(L_v/F_v, A(L_v)), \quad (15)$$

where in the right term v runs through all places of F . For each v , let \mathbb{F}_v be the residue field and let m_v be the number of components of the special fiber of the Néron model of A at v . We first note that if v split completely in L , then the cohomology group $\mathrm{H}^1(L_v/K_v, A(L_v)) = 0$. Then we apply Theorem 1.1 (for $v \in S$) together with Proposition I.3.8 of [Mil86] (for $v \notin S$ and hence unramified) to show that the index is bounded by the product $\mathbf{B}_F := \prod_{v \in S(F)} |\bar{A}(\mathbb{F}_v)_p|^{d+1} \cdot \prod_{v \notin S(F)} m_v$, where in the second product v runs through all the places not splitting completely in L . We also note that this is a finite product, since $m_v = 1$ if A has good reduction at v . Therefore, the index is finite and the first statement of Theorem 1.2 is proved. Moreover, if $d = 1$ and v_0 is a place of K not splitting completely in L , then the decomposition group of v_0 is a non-trivial closed subgroup of $\Gamma \simeq \mathbb{Z}_p$ with finite index, and hence the number of place of L sitting over v_0 is finite. This implies that the number of place of F sitting over v_0 is bounded as F varies. Therefore, the product \mathbf{B}_F is bounded, and this completes the proof of Theorem 1.2.

To prove Theorem 1.4 we use Nakayama lemma. We need to show that for each finite intermediate extension $L'/K \subset L/K$, the order of the p -torsion subgroup of $\text{coker}(\text{res}_{L'/K})$ is bounded. We apply Corollary 2.3 and use an argument similar to the above. Then we reduce the proof to showing that for each $v \in S$ at which A has split multiplicative reduction, the p -torsion subgroup of $\mathrm{H}^1(L'_v/K_v, A(L'_v))$ is bounded as L' varies. For this, we use the exact sequence

$$0 \longrightarrow Q^\mathbb{Z} \longrightarrow (L'_v)^* \longrightarrow A(L'_v) \longrightarrow 0,$$

where Q is the local Tate's period. Hilbert's theorem 90 implies that $H^1(L'_v/K_v, A(L'_v))$ is isomorphic to a subgroup of

$$H^2(\text{Gal}(L'_v/K_v), Q^{\mathbb{Z}}) \simeq H^2(\text{Gal}(L'_v/K_v), \mathbb{Z}) \simeq H^1(\text{Gal}(L'_v/K_v), \mathbb{Q}/\mathbb{Z}).$$

Obviously, the order of its p -torsion subgroup is bounded by p^d .

3. INSEPARABLE EXTENSIONS

In this section, we assume that A is an abelian variety over the local field $K = \mathbb{F}_q((T))$ so that the reduction \bar{A} of A is an ordinary abelian variety.

3.1. The dual abelian variety. Consider a finite extension L/K . The Frobenius substitution Frob_p induces a G_L -isomorphism:

$$\begin{array}{ccc} \text{Frob}_p : A(\bar{L}^{(1/p)}) & \xrightarrow{\sim} & A^{(p)}(\bar{L}) \\ P & \mapsto & F(P). \end{array} \quad (16)$$

We apply (16) to the equality (5) which, according to Corollary 2.1(c), can be written as $A^1(L^{(1/p)}) = 1/pA^1(L)$. We then use the relation (3) to deduce a new equality:

$$V((A^{(p)})^1(L)) = V(F(A^1(L^{(1/p)}))) = V(F(1/pA^1(L))) = A^1(L). \quad (17)$$

Let B denote the dual abelian variety to A over K . Being isogenous to A , B also has ordinary reduction. Let $\hat{F} : B^{(p)} \rightarrow B$ be the dual to the Frobenius isogeny F . Then the kernel of \hat{F} , which is the dual of $(\mu_p)^g$, is exactly the maximal etale subgroup of the group scheme $\mathcal{B}^{(p)}[p]$ (the kernel of the multiplication by p on $B^{(p)}$). On the other hand, if we write $[p]_B$, the multiplication by p on B , as the composition $V_B \circ F_B$, then V_B is separable and hence its kernel also equals the maximal etale subgroup of $\mathcal{B}^{(p)}[p]$. In view of these, we see that $\hat{F} = V_B \circ \Phi$, for some isomorphism $\Phi : B^{(p)} \rightarrow B^{(p)}$. In particular, we have $\hat{F}((B^{(p)})^1(L)) = V_B((B^{(p)})^1(L))$.

By letting B play the role of A in (17), we prove the following.

Lemma 3.1. *The map*

$$\hat{F} \mid_{(B^{(p)})^1(L)} : (B^{(p)})^1(L) \rightarrow B^1(L)$$

is surjective.

3.2. The local duality. Via the Poincaré biextension $W \rightarrow A \times B$ (which is the compliment of the zero section in the Poincaré line bundle over $A \times B$, [Mum68]), a point on B is regarded as an element in $\text{Ext}(A, G_m)$, and hence a point $Q \in B(L)$ gives rise to an exact sequence of G_L -modules:

$$0 \rightarrow \bar{L}^* \rightarrow W_Q \rightarrow A(\bar{L}) \rightarrow 0.$$

Using the induced long exact sequence:

$$\dots \rightarrow H^1(L, A) \xrightarrow{\delta_Q} H^2(L, \bar{L}^*) \rightarrow \dots,$$

we define (cf. [Mil86], Appendix C) the local pairing of Q and a class $\xi \in H^1(L, A)$ as

$$\langle \xi, Q \rangle_{A,B,L} := \text{inv}(\delta_Q(\xi)).$$

Here $\text{inv} : H^2(L, \bar{L}^*) \rightarrow \mathbb{Q}/\mathbb{Z}$ is the invariant of the Brauer group.

If $W_A, W_{A'}$ are Poincaré biextensions associated to A, A' and $f : A \rightarrow A'$ and $\hat{f} : B' \rightarrow B$ are dual isogenies, then $(1 \times \hat{f})^* W_A \simeq (f \times 1)^* W_{A'}$ ([Mum74], p.130). From this, we see that the local pairings are compatible with isogenies. In particular, we have the commutative diagram:

$$\begin{array}{ccc} \langle, \rangle_{A,B,L} : & H^1(L, A) \times B(L) & \longrightarrow \mathbb{Q}/\mathbb{Z} \\ & \begin{array}{ccc} F \downarrow & \uparrow \hat{F} & \parallel \end{array} & \\ \langle, \rangle_{A^{(p)}, B^{(p)}, L} : & H^1(L, A^{(p)}) \times B^{(p)}(L) & \longrightarrow \mathbb{Q}/\mathbb{Z}. \end{array} \quad (18)$$

We use (18) to deduce the following (dual statement of Lemma 3.1).

Lemma 3.2. *Let $F_* : H^1(L, A) \rightarrow H^1(L, A^{(p)})$ be the homomorphism induced from F . If $\xi \in H^1(L, A)$ and $F_*(\xi)$ annihilates $(B^{(p)})^1(L)$, then ξ must annihilate $B^1(L)$.*

We also have the commutative diagram induced from the Frobenius substitution:

$$\begin{array}{ccc} \langle, \rangle_{A,B,L^{(1/p)}} : & H^1(L^{(1/p)}, A) \times B(L^{(1/p)}) & \longrightarrow \mathbb{Q}/\mathbb{Z} \\ & \begin{array}{ccc} \text{Frob}_{p^*} \downarrow & \downarrow \text{Frob}_p & \parallel \end{array} & \\ \langle, \rangle_{A^{(p)}, B^{(p)}, L} : & H^1(L, A^{(p)}) \times B^{(p)}(L) & \longrightarrow \mathbb{Q}/\mathbb{Z}. \end{array}$$

Corollary 3.1. *Let $F_{**} : H^1(L, A) \rightarrow H^1(L^{(1/p)}, A)$ be the homomorphism induced from the inclusion $A(\bar{L}) \hookrightarrow A(\bar{L}^{(1/p)})$. If $\xi \in H^1(L, A)$ and $F_{**}(\xi)$ annihilates $B^1(L^{(1/p)})$, then ξ must annihilate $B^1(L)$.*

Proof. We observe that F_{**} is just the composition $\text{Frob}_{p^*}^{-1} \circ F_*$. \square

Using Tate's local duality theorem ([Tat62], [Mil70/72]) which says that the local pairing is non-degenerate and it identifies $H^1(L, A)$ with the Pontryagin dual of $B(L)$, we identify the annihilators of $B^1(K)$ with the dual group $\widehat{\bar{B}}(\mathbb{F}_q)$ of $\bar{B}(\mathbb{F}_q) = \bar{B}(\mathbb{F}_K)$.

Corollary 3.2. *The kernel of the homomorphism*

$$i_* : H^1(K, A) = H^1(G_K, A(\bar{K})) \rightarrow H^1(G_K, A(\bar{K}^{(1/p^\infty)}))$$

induced from the inclusion $A(\bar{K}) \rightarrow A(\bar{K}^{(1/p^\infty)})$ is contained in $\widehat{\bar{B}}(\mathbb{F}_q)$.

Proof. The corollary is proved by inductively applying Corollary 3.1 to the cases where $L = K^{(1/p^m)}$ for $m = 0, 1, \dots$ \square

Note: It can be shown that the kernel actually equals $\widehat{\bar{B}}(\mathbb{F}_q)$, but we do not need it here.

3.3. Kummer theory. Over the field $\bar{K}^{(1/p^\infty)}$, we are able to establish the related Kummer theory, because we have the exact sequence of G_K -modules

$$0 \longrightarrow A[p^m] \xrightarrow{j} A(\bar{K}^{(1/p^\infty)}) \xrightarrow{[p^m]} A(\bar{K}^{(1/p^\infty)}) \longrightarrow 0.$$

Furthermore, in the exact sequence we can replace $A[p^m]$ by $\bar{A}[p^m]$ (Lemma 2.1). By taking the direct limit over m of the induced Kummer sequence, we get the following exact sequence:

$$A(K^{(1/p^\infty)}) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p \hookrightarrow H^1(G_K, \bar{A}[p^\infty]) \xrightarrow{j_*} H^1(G_K, A(K^{(1/p^\infty)}))_p$$

where $H^1(G_K, A(K^{(1/p^\infty)}))_p$ denotes the p -primary part of the group $H^1(G_K, A(K^{(1/p^\infty)}))$. Now equations (5) and (6) together actually imply

$$A(K^{(1/p^\infty)}) \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p = A(K^{(1/p^\infty)})_p \otimes_{\mathbb{Z}} \mathbb{Q}_p/\mathbb{Z}_p = 0. \quad (19)$$

If we set $k_* = j_*^{-1} \circ i_* : H^1(K, A)_p \longrightarrow H^1(G_K, \bar{A}[p^\infty])$, then, by Corollary 3.2,

$$\ker(k_*) \subset \widehat{\bar{B}}(\mathbb{F}_q) \quad (20)$$

3.4. The proof of Theorem 1.1. First, we restrict the map k_* to the finite p -group $H^1(L'/K, A(L'))$. Because of the inclusion (20), the kernel is also contained in $\widehat{\bar{B}}(\mathbb{F}_q)_p$ whose order equals $|\bar{A}(\mathbb{F}_q)_p|$. On the other hand, by applying the equality (19) (for the case where $K = L'$), we can deduce that the image is contained in $H^1(\text{Gal}(L'/K), \bar{A}(\mathbb{F}_{L'})_p)$. According to Corollary 2.1(e), the $\text{Gal}(L'/K)$ -module $\bar{A}(\mathbb{F}_{L'})_p$ equals $A(L'^{(1/p^m)})_{\text{tor}, p}$ for large enough m . In view of this, Corollary 2.2 implies

$$|H^1(\text{Gal}(L'/K), \bar{A}(\mathbb{F}_{L'})_p)| \leq |A(K^{(1/p^m)})_{\text{tor}, p}|^d = |\bar{A}(\mathbb{F}_q)_p|^d.$$

And the proof is completed.

REFERENCES

- [BL06] A. Bandini and I. Longhi, *Control theorems for elliptic curves over function fields*, to appear in the International Journal of Number Theory.
- [CoG96] J. Coates, R. Greenberg, *Kummer theory for abelian varieties over local fields*, Invent. math. **124**(1996), 129-174.
- [Gre03] R. Greenberg, *Galois theory for the Selmer group for an abelian variety*, Compositio Math. **136**(2003), 255-297.
- [KaT03] K. Kato, F. Trihan, *On the conjecture of Birch and Swinnerton-Dyer in characteristic $p > 0$* , Invent. Math. **153**(2003), 537-592.
- [Maz72] B. Mazur, *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18**(1972), 183-266.
- [Mil70/72] J.S. Milne, *Weil-Chatelet groups over local fields*, Ann. Sci. Ecole Norm. Sup. **3** (1970), 273-284; *ibid.*, **5** (1972), 261-264.
- [Mil80] J.S. Milne, *Étale Cohomology*, Princeton University press, Princeton, 1980.
- [Mil86] J.S. Milne, *Arithmetic duality theorems*, Academic Press, New York, 1986.
- [Mum68] D. Mumford, *Biextension of formal groups*, in the proceedings of the Bombay Colloquium on Algebraic Geometry, Tata Institute of Fundamental Research Studies in Mathematics 4, London, Oxford University Press 1968.

- [Mum74] D. Mumford, *Abelian Varieties*, Oxford Univ. Press, 1974.
- [OTr06] T. Ochiai, F. Trihan, *On the Selmer groups of abelian varieties over function fields of characteristic $p > 0$* , to appear in Mathematical Proceedings Cambridge Philosophical Society.
- [OTr08] T. Ochiai, F. Trihan, *On the Iwasawa main conjecture of abelian varieties over function fields of characteristic $p > 0$* , manuscript 2008.
- [Sha72] S. Shatz, *Profinite Groups, Arithmetic, and Geometry*. Annals of Math. Studies **67**, Princeton University Press, Princeton , 1972.
- [Tat62] J. Tate, *Duality theorems in Galois cohomology over number fields*, Proc. Intern. Congress Math. Stockholm, 234-241.
- [Tat67] J. Tate, *Global Class Field Theory*. In Algebraic Number Theory, J.W.S. Cassels and A. Frölich, eds., Academic Press, 1967, 162-203.
- [Was82] L. Washington, *Introduction to Cyclotomic Fields*, Springer-Verlag, 1982.

DEPARTMENT OF MATHEMATICS, NATIONAL TAIWAN UNIVERSITY, TAIPEI
10764, TAIWAN

E-mail address: `tan@math.ntu.edu.tw`